UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/621,060	07/21/2000	Dennis K. Branstad	NAI1P078/99.042.02	4286

28875 7590 03/11/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
ZIA, MOSSADEQ	

ART UNIT	PAPER NUMBER
2134	9

DATE MAILED: 03/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/621,060	BRANSTAD ET AL.	
	Examiner	Art Unit	
	Mossadeq Zia	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 14, 16-18, 19, 21-23 are rejected under 35 U.S.C. 102(b) as anticipated by Venkatesan et al, "Threat-Adaptive Security Policy".

3. **Regarding** claim 14, Venkatesan disclose a method for authenticating information to be exchanged between a sender and a receiver, comprising:

identifying a change in a parameter (security policy) that affects a selection of an authentication strength level (level of trust) between a sender and a receiver; and

dynamically modifying (run-time and decide) said authentication strength level based upon said identified change (Venkatesan, pg. 526, col. 1, para. 1, line 3-5).

4. **Regarding** claim 16, Venkatesan discloses the method of claim 14 above, and further disclose wherein step (a) comprises identifying a change in authentication error level (Venkatesan, pg. 526, col. 1, para. 2, line 13-17).

5. **Regarding** claim 17, Venkatesan discloses the method of claim 14 above, and further disclose wherein step (a) comprises receiving a network defense alarm (flagged, Venkatesan, pg. 529, col. 2, last para.).

6. **Regarding** claim 18, Venkatesan discloses the method of claim 14 above, and further disclose wherein step (a) comprises identifying a change in security policy (Venkatesan, pg.527, col. 1, section 3.1, line 8-10).

7. **Regarding** claim 19, Venkatesan disclose a method for authenticating information to be exchanged between a sender and a receiver, comprising:

selecting a first authentication mechanism from among a plurality of authentication mechanisms that collectively define at least two different authentication strength and performance tradeoffs (Figure 1); and

dynamically switching from said first authentication mechanism to a second authentication mechanism in said plurality of authentication mechanisms in response to a change in a monitored condition (Venkatesan, pg. 526, col. 1, para. 1, line 3-5).

8. **Regarding** claim 21, Venkatesan discloses the method of claim 19 above, and further disclose wherein step (b) comprises switching to said second authentication mechanism (more secure state) upon a change in authentication error level (Venkatesan, pg.527, col. 2, section 3.2, line 12-18).

9. **Regarding** claim 22, Venkatesan disclose the method of claim 19 above, and further disclose wherein step (b) comprises switching to said second authentication mechanism upon receipt of a network defense alarm (Venkatesan, pg.528, col. 1, section 3.3, line 2-5).

10. **Regarding** claim 23, Venkatesan disclose the method of claim 19 above, and further disclose wherein step (b) comprises switching to said second authentication mechanism upon a change in security policy (Venkatesan, pg.527, col. 1, section 3.1, line 8-10, col. 2, section 3.2, line 7-8, 12-14).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1, 5-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Samar et al., "Unified Login with Pluggable Authentication Modules (PAM)" by Samar et al in view of "Design and Implementation of Modular Key Management Protocol and IP Secure Tunnel on AIX" by Cheng et al.

13. **Regarding** claims 1, 11, Samar et al discloses a system for authenticating message data to be exchanged between a sender and a receiver, comprising:

a controller (API, Samar, page 1, para. 5, line 3) that dynamically selects one of a plurality of authentication mechanisms (authentication services, Samar, page 1, para. 5, line 4) to be used in providing authentication for an exchange of message data (response, Samar, page 3, 2nd to last para., last sentence);

but fail to show:

a security association and key management module that establishes security associations for said plurality of authentication mechanisms; and

an authentication module that includes support for said plurality of authentication mechanisms, wherein said authentication module generates an authentication tag using an authentication mechanism selected by said control, said authentication tag being appended to said message data.

However, Cheng et al. show a key management system, which teaches that security association between two communicating systems represents the information shared by systems in order to control a secure communication between them (security associations,). This information includes secret keys, key life-times, nonces, crypto algorithms, parameters, etc., (Cheng, page 1, introduction, col. 1, last 3 sentences, col. 2, 1st sentence). Further more, Cheng teaches a Message Authentication Code (tag) [or integrity check function] which is applied to a piece of information (message data) for authentication (Cheng, page 3, section 2.1.1, col. 2, definition MAC_k, figure 4).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Samar et al as per teaching of Cheng et al such that the key management system will provide secure communication over the currently insecure Internet (Cheng, page 1, introduction, col. 1, para. 2, lines 2-3).

14. **Regarding** claim 5, Samar and Cheng disclose the system of claim 1 above, and further disclose wherein said controller receives an input identifying a security policy (Cheng, list, policy cache, page 7, col. 1, para. 2, line 4).

15. **Regarding** claim 6, Samar and Cheng disclose the system of claim 1 above, and further disclose wherein said controller includes a network security service resource (policy engine, Cheng, pg. 6, col. 2, section 3.2, para. 1, line 2-4) and one or more security association resource managers contexts (policy cache, Cheng, pg. 6, col. 2, section 3.2, para. 1, line 6-8), each of said one or more security resource managers contexts being established for a corresponding network application (SAID, Cheng, pg. 10, col. 1, para. 1, line 13) and being responsible for establishing and maintaining an authentication mechanism for a corresponding associated network

application (secure communication, Cheng, page 10, col. 2, 1st bullet), said network security service resource being responsible for providing resource and security constraints within which each of said one or more security resource managers contexts operates (Cheng, pg. 7, col. 2, para. 1, line 1-2, 6-7).

16. **Regarding** claim 7, Samar and Cheng disclose the system of claim 1 above, and further disclose wherein said security association and key management module generates an authentication key for authenticating said message data (message authentication key, Cheng, page 5, col. 1, last paragraph, line 1-4).

17. **Regarding** 8, Samar and Cheng disclose the system of claim 1 above, and further disclose wherein said security association and key management module generates a confidentiality key for securing control messages (session key, pg. 3 section 2.1.1, 1st paragraph, line 1-4).

18. **Regarding** claim 9, Samar and Cheng disclose the system of claim 1, and further disclose wherein said security association and key management module operates in accordance with the Internet Key Exchange standard (see IKE RFC, introduction referring phase 1&2, Cheng, page 2, col. 1, line 1, 7-9 discusses similar idea).

19. **Regarding** claim 10, Samar and Cheng disclose the system of claim 1 above, and further discloses said authentication module operates in accordance with the IPsec standards (Cheng, page 2, col. 1, 2nd to last paragraph, page 4, section 2.2, col. 1).

20. **Regarding** claim 12, Samar and Cheng disclose claim 1 above, and further discloses a security association and key management module that establishes and maintains said plurality of authentication mechanisms (crypto algorithms, Cheng, pg. 8, Figure 8).

21. Claims 2, 13 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Samar et al., "Unified Login with Pluggable Authentication Modules (PAM)" in view of "Design and Implementation of Modular Key Management Protocol and IP Secure Tunnel on AIX" by Cheng et al. in further view of "Throughput Improvement Through Dynamic Load Balance" by More et al.

22. **Regarding** claim 2, Samar et al. and Cheng et al. discloses the system of claim 1 above, but fails to disclose wherein said controller receives an input identifying a processor load.

However, More et al. teaches link-fault-tolerant algorithm (controller) that solves branch and bound problem using hyper-cubes. If the hypercube has link faults, special measures (identifying a processor load) need to be taken to balance the load (More, pg. 339. col. 1, Abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Samar et al. and Cheng et al. as per teaching of More et al. to include load dynamic balance to improve the performance of a multiprocessor system by allocating tasks such that all the processor are evenly loaded (More, pg. 339. col. 1, Abstract).

23. **Regarding** claim 13, Samar and Cheng discloses the system of claim 2 above, and further disclose wherein said security association and key management module operates in accordance with IKE (see IKE RFC, introduction referring to phase 1&2, Cheng, page 2, col. 1, line 1, 7-9 discusses similar 2 phase idea).

24. Claims 3, 4 are rejected under **35 U.S.C. 103(a)** as being unpatentable over Samar et al., "Unified Login with Pluggable Authentication Modules (PAM)" in view of "Design and

Implementation of Modular Key Management Protocol and IP Secure Tunnel on AIX" by Cheng et al. in further view of "Threat-Adaptive Security Policy" by Venkatesan et al.

25. **Regarding** claim 3, Samar and Cheng discloses the system of claim 1 above, but fail to further disclose said controller receives an input identifying an authentication error level.

However, Venkatesan et al. teach Threat-Adaptive model where the level of authentication required increases with the increase of perceived threat from the user (Venkatesan, pg. 526, col. 1, para. 2, line 13-17).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Samar et al. and Cheng et al. as per teaching of Venkatesan et al. to include Threat-Adaptive model which adaptively varies the security constraints for each user, thereby improving the system performance (Venkatesan, pg. 525, col. 1, Abstract, last line).

26. **Regarding** claim 4, Samar and Cheng disclose the system of claim 1 above, and further disclose wherein said controller receives an input identifying network defense alarms.

However, Venkatesan et al. teach Threat-Adaptive monitors each user's activities. For a malicious user, the system would counter with the most rigid set of security constraints (identifying network defense alarms, Venkatesan, pg. 526, col. 1, para. 3, line 1, 4-6). Further more any deviation is flagged as a potential threat to the system (flagged, Venkatesan, pg. 529, col. 2, last para.).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Samar et al. and Cheng et al. as per teaching of Venkatesan et al. to include Threat-Adaptive model which adaptively varies the security constraints for each user, thereby improving the system performance (Venkatesan, pg. 525, col. 1, Abstract, last line).

27. Claims 15, 20 are rejected under **35 U.S.C. 103(a)** as being unpatentable over "Threat-Adaptive Security Policy" by Venkatesan et al. in view "Throughput Improvement Through Dynamic Load Balanace" by More et al.

28. **Regarding** claim 15, Venkatesan et al. discloses the method of claim 14 above, but fail to disclose wherein step (a) comprises identifying a change in processor load.

However, More et al. teaches link-fault-tolerant algorithm (controller) that solves branch and bound problem using hyper-cubes. If the hypercube has link faults, special measures (identifying a processor load) need to be taken to balance the load (More, pg. 339. col. 1, Abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Venkatesan et al. as per teaching of More et al. to include load dynamic balance to improve the performance of a multiprocessor system by allocating tasks such that all the processor are evenly loaded (More, pg. 339. col. 1, Abstract).

29. **Regarding** claim 20, Venkatesan et al. discloses the method of claim 19 above, but fail to disclose wherein step (b) comprises switching to said second authentication mechanism upon a change in processor load.

However, More et al. teaches link-fault-tolerant algorithm (controller) that solves branch and bound problem using hyper-cubes. If the hypercube has link faults, special measures (identifying a processor load) need to be taken to balance the load (More, pg. 339. col. 1, Abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Venkatesan et al. as per teaching of More et al. to include load dynamic

balance to improve the performance of a multiprocessor system by allocating tasks such that all the processor are evenly loaded (More, pg. 339. col. 1, Abstract).

Conclusion

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mossadeq Zia
Examiner
Art Unit 2134

mz
3/3/04

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100